(12) EUROPEAN PATENT APPLICATION

(72) Inventors:
• Martin, Jean-Christophe
  38760 Varces (FR)
• McKinty, Steve
  38570 Theys (FR)

(74) Representative:
de Beaumont, Michel
1, rue Champollion
38000 Grenoble (FR)

(54) Network link bypass device

(57) For bypassing a computer system coupled
between first and second network links, the computer
system executes a software which provides a predeter-
mined control signal on a control line. The control line is
polled by a bypass device that will cause the computer
system to be bypassed when said control signal is not
present on the control line. The control signal may be in
the form of periodic pulses and a bypassing is caused
when a pulse is not received on the control line within a
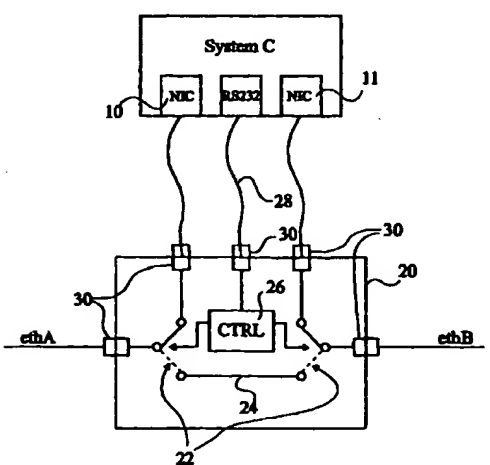predetermined period of time.

Fig 2

EP 0 949 789 A1

Description

[0001]　The present invention relates to a device for bypassing a computer system interconnecting two network links when this computer system fails.

[0002]　It is often desirable to insert, between two systems interconnected through a network link, a transparent control system for various possible purposes. The control system may be used for restricting access, for event logging, for ciphering and deciphering...

[0003]　Figure 1 schematically shows an arrangement providing this functionality. A system A normally communicates with a system B over a network link, such as an Ethernet link. A control system C is inserted in the network link between systems A and B. In other words, system A is coupled to a network interface card 10 of system C through a network link ethA, while system B is coupled to a second network interface card 11 of system C through a network link ethB.

[0004]　System C, usually a work station, is supposed to be transparent for systems A and B as regards the network frames exchanged between them. For this purpose, system C executes software which copies the frames between links ethA and ethB. In fact, it mainly operates as a hub. In some cases, however, the software may analyze the frames or even perform operations thereon.

[0005]　Of course, system C is subject to failure. In case of failure, it is desirable to maintain the link between system A and system B. For this purpose, it is known to use bypass devices which are capable of detecting a hardware failure, for example by achieving CRC checks on the frames, in order to switch the network links to bypass links.

[0006]　However, such devices are not able to detect a software failure, such as an abnormal program termination or a system hang. Indeed, in this case, the frames do not have errors, they are simply not copied from one link to the other.

[0007]　An object of the present invention is to provide a bypass device capable of achieving its function in case of a software failure of a control system.

[0008]　This object and others are achieved by executing on the transparent system a software which provides a predetermined control signal on a control line. The control line is polled by the bypass device. The bypass device will bypass the transparent system when the control signal is not present on the control line.

[0009]　According to a preferred embodiment of the invention, the control signal is in the form of periodic pulses and a bypassing is caused when a pulse is not received on the control line within a predetermined period of time.

[0010]　The bypass device includes a switch having a first position selecting a main path between first and second network links, including the transparent system, and a second position selecting a bypass path between the first and second network links. A control circuit selects the first position of the switch when the control signal is received on the control line, and selects the second position of the switch when the control signal is not received on the control line.

[0011]　The foregoing and other objects, features, aspects and advantages of the invention will become apparent from the following detailed description of embodiments, given by way of illustration and not of limitation with reference to the accompanying drawings.

　　　Figure 1, previously described, shows a conventional arrangement including a transparent control system inserted in a network link;
　　　Figure 2 shows an embodiment of a network bypass device according to the invention; and
　　　Figure 3 shows another embodiment of a network bypass device according to the invention.

[0012]　A network bypass device according to the invention is intended to reestablish the network link between systems A and B of figure 1 in case of a software failure in transparent control system C.

[0013]　Figure 2 schematically shows an embodiment of such a device. The device 20 is connected between control system C and the two network links ethA and ethB. It includes a double switch 22 which, in a first and normal position, connects network link ethA to network interface card 10 of system C and connects network link ethB to network interface card 11 of system C. Thus, in its normal position, switch 22 connects system C to the network links ethA and ethB exactly as in figure 1.

[0014]　In a second, bypass position, shown in dotted lines, switch 22 connects network links ethA and ethB directly the one to the other through a link 24.

[0015]　Switch 22 is operated by a control circuit 26 which is coupled to system C through a control line 28.

[0016]　The software executed by system C is adapted to provide a specific control signal on line 28. As long as this control signal is present on line 28, control circuit 26 selects the normal position of switch 22, so that the traffic on links ethA and ethB normally passes through system C.

[0017]　In the case of a software failure, the software is no longer capable of providing the control signal on line 28. Control circuit 26 detects the absence of the control signal and, as a consequence, selects the bypass position of switch 22, directly interconnecting links ethA and ethB through link 24.

[0018]　The control signal generated by the software on line 28 is, for example, in the form of periodic pulses. Control circuit 26 then includes a timer which restarts counting down a time-out period at each arrival of a pulse. If a pulse does not arrive because of a software failure, the timer reaches the time-out period and selects the bypass position of switch 22.

[0019]　Of course, if the hardware of system C fails, the software will also fail in many cases, whereby the device according to the invention will also perform its bypass

function.

[0020]   In a preferred embodiment, as shown, the bypass device 20 is external to system C. Device 20 is then included in a housing provided with standard connectors 30 which directly receives the network links ethA and ethB and enable system C to be coupled to device 20 through standard cables. Control line 28 is then any externally available standard link, such as a serial RS232 link, as shown. It is particularly simple to send any specific signal on a standard serial link by software.

[0021]   An RS232 link has the additional advantage of providing supply voltages, which may be used for powering the bypass device 20. However, an independent powering of the bypass device will allow the device to continue operating even if system C has a power failure.

[0022]   Figure 3 shows another embodiment of a network bypass device according to the invention, here designated by 20'. In figure 3, same elements as those in figure 2 are designated with same reference characters.

[0023]   One difference of this embodiment with respect to that of figure 2 is that the direct bypass link 24 of figure 2 is replaced by two connectors 32 which are respectively internally connected to links ethA and ethB through switch 22 when it is in its bypass position (dotted lines).

[0024]   Each of connectors 32 is intended to be coupled to a respective network interface card of a second, backup system C which performs the same functions as system C.

[0025]   With this arrangement, when main system C fails, bypass device 20' interconnects network links ethA and ethB through backup system C. This embodiment is particularly useful if system C performs important security functions.

[0026]   Of course backup system C may be replaced by a direct external link between connectors 32, whereby the device will operate as that of figure 2.

[0027]   In some cases, network interface cards are connected to their respective links through transceivers which adapt the physical interface of the network cards to the characteristics of the network links. A bypass device according to the invention, as shown in figure 3, may advantageously include such transceivers. As shown, the transceivers 34 are inserted between switch 22 and respective connectors 30.

Claims

1. A device for interconnecting a first network link (ethA), a second network link (ethB) and a computer system (C) that transfers information between the first and second network links under the control of a software executed by the computer system, characterized in that it includes:

    a switch (22) having a first position selecting a

main path between the first and second network links, including said computer system, and a second position selecting a bypass path between the first and second network links; and

    a control circuit (26) for selecting the first position of the switch when a predetermined control signal is received on a control line (28) coupled to said computer system, and for selecting the second position of the switch when the predetermined control signal is not received on the control line;

    wherein said software is adapted to provide the predetermined control signal on the control line.

2. The device of claim 1, wherein said predetermined control signal is in the form of periodic pulses, the control circuit being arranged to select the second position of the switch when a pulse of the control signal has not been received within a predetermined period of time.

3. The device of claim 1, wherein the control line is a standard serial link between the device and the computer system.

4. The device of claim 1, wherein said bypass path includes a direct link.

5. The device of claim 1, wherein said bypass path includes a backup computer system.

6. The device of claim 1, included in an external housing and comprising:

    first and second connectors for respective connection to the first and second network links;
    third and fourth connectors in said main path for respective connection to two network interface cards of the computer system; and
    a fifth connector for connection of the control line.

7. The device of claim 6, comprising sixth and seventh connectors in said bypass path for respective connection to two network interface cards of a backup computer system.

8. The device of claim 6, wherein said main path includes a transceiver connected to each of the third and fourth connectors inside said housing.

9. A method for bypassing a computer system (C) coupled between first and second network links (ethA, ethB), characterized in that it includes the steps of:

executing in said computer system a software
which provides a predetermined control signal
on a control line;

polling the control line; and

bypassing the computer system when said
control signal is not present on the control line.

10. The method of claim 9, wherein said control signal
    is in the form of periodic pulses and the step of poll-
    ing includes expecting a pulse on the control line
    within a predetermined period of time.
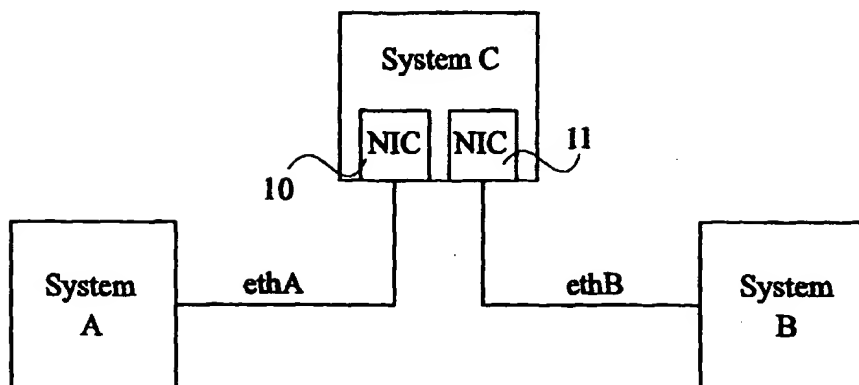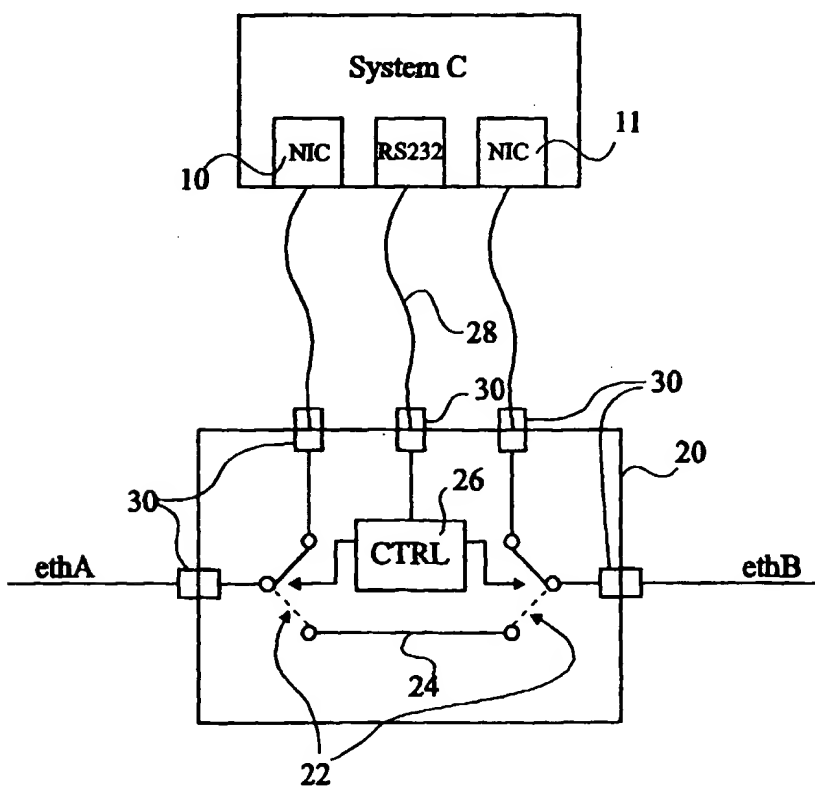
5

10

15

20

25

30

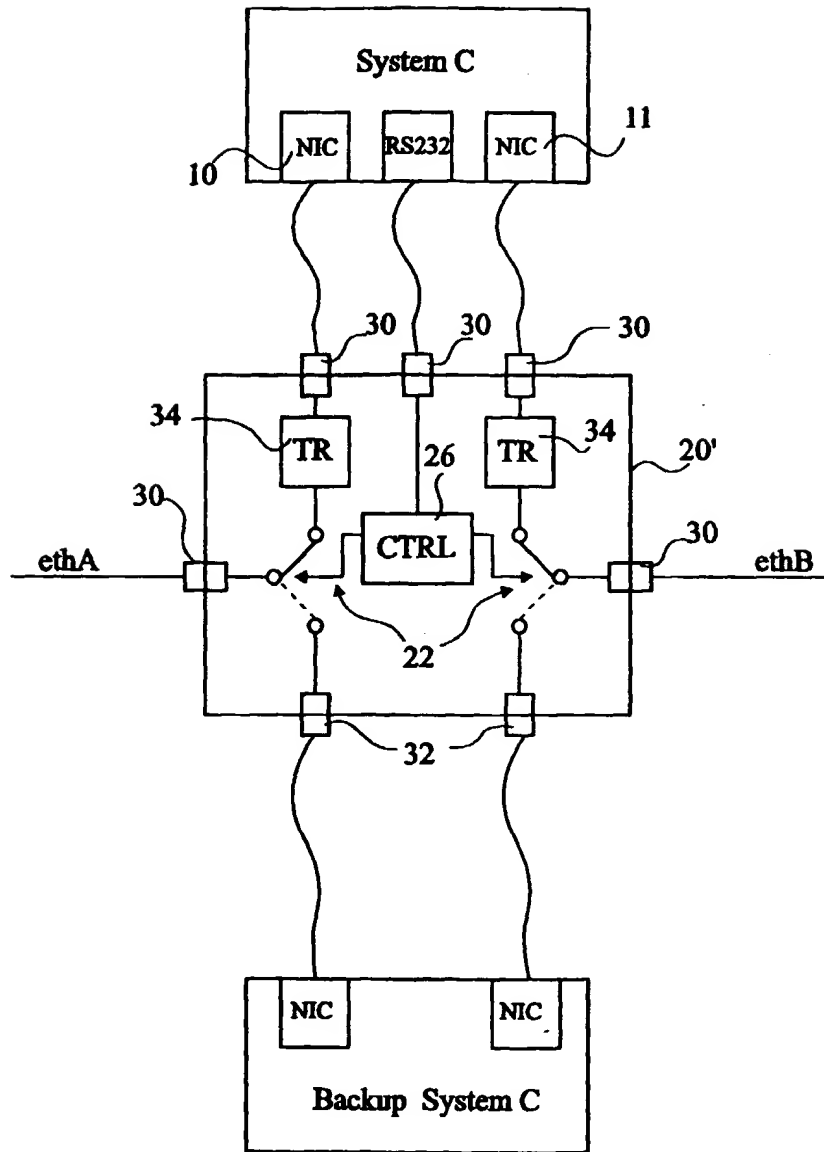35

40

45

50

55

Fig 1

Fig 2

Fig 3

	European Patent Office	EUROPEAN SEARCH REPORT	

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
Y	US 5 317 198 A (HUSBANDS CHARLES R) 31 May 1994 * column 1, line 9 - line 44 * * column 3, line 35 - column 4, line 17 * * figure 1 *	1,2,4,6,9,10	H04L29/14 H04L12/413
Y	EP 0 397 196 A (ALCATEL NV) 14 November 1990 * page 2, column 1, line 1 - line 22 * * page 2, column 2, line 34 - line 36 * * page 5, column 7, line 1 - column 8, line 43 *	1,2,4,6,9,10	
A	PATENT ABSTRACTS OF JAPAN vol. 098, no. 006, 30 April 1998 & JP 10 051479 A (HITACHI DENSHI LTD), 20 February 1998 * abstract *	1,4,9	
A	US 5 677 838 A (ITOU KEIJI ET AL) 14 October 1997 * abstract * * column 1, line 53 - column 2, line 10 * * column 2, line 44 - column 3, line 5 * * column 4, line 15 - line 26 * * claims 1,4 *	1,2,9,10	TECHNICAL FIELDS SEARCHED (Int.Cl.6) H04L G06F

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	4 September 1998	Karavassilis, N

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.

EP 98 41 0037

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report.
The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

04-09-1998

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
US 5317198	A	31-05-1994	NONE		
EP 0397196	A	14-11-1990	US 4964095 A		16-10-1990
			AT 118136 T		15-02-1995
			AU 625847 B		16-07-1992
			AU 5468790 A		15-11-1990
			CA 2016638 A,C		12-11-1990
			DE 69016493 D		16-03-1995
			DE 69016493 T		29-06-1995
			ES 2070947 T		16-06-1995
US 5677838	A	14-10-1997	JP 7291091 A		07-11-1995
			DE 19515190 A		02-11-1995